

January 19, 2007

Federal Trade Commission/Office of the Secretary, Room H-135
Identity Theft Task Force - P 065410
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

RESPONSE TO FEDERAL TRADE COMMISSION'S REQUEST FOR PUBLIC COMMENT REGARDING PRESIDENT BUSH'S ID THEFT TASK FORCE

First Data Corporation appreciates the opportunity to comment on the questions posed by the President's Federal Identity Theft Task Force as the members develop recommendations to combat the critical issue of identity theft. Our comments focus on private sector uses of Social Security Numbers (SSNs), national data security standards, breach notice requirements for private sector entities, education of the private sector and consumers, and law enforcement.

By way of background, First Data is a Denver-based financial services firm that is the leading processor of electronic payment transactions. As a Fortune 500 company that employs over 29,000 employees globally, our services help consumers, businesses and governmental entities make payments for goods and services using virtually any form of payment: credit card; debit and stored value card; electronic checks and paper checks at the point of sale; and over the Internet. In addition, First Data owns and operates the STAR® Network, which is a coast-to-coast electronic payments network.

I. Maintaining Security of Consumer Data

2. Comprehensive Record on Private Sector Use of SSNs

The Task Force, in seeking to address the extent to which the availability of SSNs to identity thieves creates the possibility of harm to consumers, is considering whether to recommend that the Task Force investigate and analyze how SSNs are currently used in the private sector, and how these uses could be modified or limited to help minimize the unnecessary exposure of SSNs and/or to make them less valuable in committing identity theft. Would such an effort be helpful in addressing the problem of identity theft? To what extent would such an effort be the appropriate way to gather this information?

The SSN has become a ubiquitous data element in both the public and private sectors in the U.S. While we believe it is prudent for the Task Force to investigate and analyze how and whether to limit widespread access to, and use of, consumers' SSNs to combat identity theft, it is critical to understand that there are legitimate uses for SSNs, particularly within the payments sector. In fact, policies seeking to protect SSNs by limiting their legitimate uses (e.g. fraud prevention purposes) would actually make it easier to commit ID theft, fraud or other criminal activities.

With thousands of financial transactions occurring every second, effective fraud prevention and risk management depend on the ability to match a range of information about a consumer to ensure that identity theft or other forms of fraud are not being committed. The SSN is the most

important data element because it is the *only* reliable, unique identifier that never leaves a person; phone numbers, driver's license numbers, account numbers, addresses and other forms of identification change over time. The inability to use SSNs to link disparate data about a consumer would lead to an increase in inaccurate data and ultimately more fraud and less reliable risk management tools. The consumer will pay the price as the cost of credit and insurance and the inconvenience of applying for them increase accordingly.

SSNs are relied upon by the financial services industry as a primary identifier of consumers. They help validate key questions financial institutions ask, such as "is the person who they say they are;" and "is this person, with this SSN, authorized to transact on this account?" Specifically, First Data and our customers rely on full, 9-digit SSNs to (1) detect, deter and stop fraud, and (2) enforce transactions that have been initiated by the consumer:

- Fraud Prevention: in cases of fraud, it is common for multiple names to be associated with one particular SSN. Our fraud prevention systems allow us to look up an SSN and tie a name search or an address search to it. If multiple names are returned with one SSN, it might indicate that fraud is being committed. Additionally, by researching address history (linked primarily by SSNs), our customers can determine if a family member is committing fraud against another family member.
- Stolen Cards: If a consumer reports a stolen card, "out of wallet" questions are key to ensuring that it is the victim calling rather than the criminal trying to reactivate a card using information found in a wallet. The answers to these questions are found by tying the SSN to various public data.
- Verification for New Accounts: the SSN is used to confirm the identity of individuals attempting to open an account at a financial institution.
- Debt Collection: If an individual skips out on his/her debts and moves around the country in an effort to evade collectors, the SSN is the best identifier that can be used to track the debtor despite multiple addresses, state driver's licenses and name changes.

3. National Data Security Standards

The Task Force is considering whether to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. Would such national requirements be helpful in addressing any deficiencies in current data security practices? If so, what would be the essential elements of such a requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size? On a related note, please provide any comments that you may have on the costs of imposing a national data security requirement on businesses.

If the Task Force were to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information, we contend that such a requirement should not mandate a one-size-fits-all approach and should not be too prescriptive. A generalized approach, by its nature, would not take into account the differences in the way various commercial entities and industries currently safeguard sensitive consumer information. Furthermore, any data security requirements imposed on commercial entities should also be imposed on public sector entities that maintain sensitive consumer information because Americans should expect the same levels of protection of their sensitive consumer information, regardless of whether it is maintained by a commercial entity or in the public sector.

For years, First Data has been on the front lines fighting fraud and identity theft. In our experience criminals have become highly sophisticated in their efforts to perpetrate fraud. As a result, we firmly believe that imposing specific government mandates on administrative, technical and physical safeguards on the private sector would hinder our ability to develop and implement new or creative technologies and methodologies that could help enhance the security of consumer's personal information and combat ID theft.

The federal banking regulators have already implemented comprehensive rules, procedures and processes for the financial services industry that are a good model for other industries. Currently, financial institutions can look to the Federal Financial Institutions Examination Council's (FFIEC) Information Security Booklet when developing and implementing their information security programs. As written in the FFIEC IT Handbook Executive Summary, "the safety and soundness of the financial industry and the privacy of customer information depend on the security practices of banks, thrifts, credit unions and their service providers. The Information Security Booklet describes how an institution should protect the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers to maintain effective programs *tailored to the complexity of their operations* [emphasis added]."¹

Additionally, the current Payment Card Industry Data Security Standard, developed by VISA, MasterCard, American Express, Discover and JCB, creates a comprehensive security standard that is intended to help the payments industry and merchants proactively protect customer account data. (www.pcisecuritystandards.org).

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

The Task Force is considering whether to recommend that a national breach notification requirement be adopted. Would such a breach notification requirement be helpful in addressing any deficiencies in the protocols currently followed by businesses after they suffer a breach? If so, what would be the essential elements of such a national breach notification requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size?

Entities like First Data that own, license, maintain or have access to personal information are subject to 34 state laws (including Washington, D.C.'s recently enacted law) that are anything but consistent. The states vary in their definition of a security breach, the personal information that should be covered, the type of breach that triggers notification, the timing of the notification, content of the notice and method of the notice.

First Data strongly believes that consumers should be notified when their personal information has become compromised - and that it is in the best interest of businesses and consumers to have a uniform, national standard - but we urge the Task Force members to avoid recommending a national standard that fails to take into account the various industry players and myriad roles they play. Failure to do so may create a situation where, despite the best of their abilities or intentions, certain entities simply will not be able to comply.

Additionally, as part of this public dialogue, we encourage the Task Force to consider "identity fraud" differently from "card fraud." Identity theft was broadly defined in the Identity Theft and

¹ FFIEC Information Technology Examination Handbook Executive Summary, page 3, <http://www.ffiec.gov/ffiecinfbase/booklets/HandbookExecutive%20SummaryFinalDraft10.pdf>

Assumption Deterrence Act of 1998 to include knowingly using means of identification to commit unlawful activity. In practice, the financial services industry delineates between the various forms that “identity theft” can take. For example, our industry considers identity fraud to be when a criminal opens lines of credit and accounts by assuming another person’s identity, typically with the aid of the victim’s SSN. Card fraud, on the other hand, occurs when a criminal has obtained a credit or debit card number and buys goods and services using that card number. While debit card fraud, in particular, may have an immediate impact on a consumer because the money can be withdrawn immediately, it is ultimately not as grave a risk as identity fraud. Federal law and regulation (under the Electronic Funds Transfer Act and Regulation E) provide many protections for consumers engaging in electronic funds transfers, including error resolution and a maximum liability of \$50 for unauthorized charges. And unlike information acquired in identity fraud, a debit or credit card number obtained through fraudulent means cannot be used to open a new checking or savings account. Identity fraud also poses more serious problems to consumers because clearing their name and credit records can take considerable time and personal effort.

In the Federal Reserve Bank of Philadelphia’s discussion paper on identity theft, it states, “Despite the legal definition of identity theft, there are important distinctions among these crimes, including their potential to result in financial losses for consumer-victims and bank lenders. Applying the broad definition of identity theft makes it difficult to quantify financial costs, incidence rates and criminal arrest rates associated with the sub-categories of identity theft. This data affects financial institutions when they evaluate the effectiveness of countermeasures targeting specific financial frauds. It affects law enforcement when assessing whether these types of financial frauds are increasing or decreasing and the implications of such trends. Also, it affects policymakers attempting to identify appropriate legislative or regulatory remedies to these various crimes. Perhaps most important, the data gap affects consumers’ ability to accurately assess their relative risk of becoming a victim or, if they are victims, their potential financial and other losses. As a result, consumers may alter behaviors to protect against the most harmful form of identity theft, true name fraud, rather than matching their precautions to specific threats. For example, applying an overly broad definition may result in unintended consequences such as creating unwarranted fears among consumers about using electronic payments and commerce.”²

In the two years’ worth of breaches that have been made public, very few of those have been linked to identity fraud. When asked about the fear about security breaches, Professor Fred H. Cate, distinguished professor of law at Indiana University and director of Indiana University’s Center for Applied Cybersecurity Research replied, “...identity theft is not occurring with the frequency we often hear about in the press; in fact, studies suggest it is actually declining.”

Professor Cate went on to say, “...the notification laws have created an incentive to improve data protection and housekeeping for consumer and employee information. But these state notification laws have caused problems too. The public has been inundated with notices where frankly little risk was presented and where there was little they could do in any event. Moreover, some state legislatures think they have solved the ID theft problem by passing these laws, and that’s all they have to do. To the extent that these laws are leaving other problems unaddressed, this is a major concern. First, all the data we have now tell us that the biggest threat to our personal information security is the people we know. It’s the same with many violent crimes. Most ID theft is committed by people you know. So laws that focus on strangers -- such as notification laws -- actually misfocus our attention. It would be better to tell people to lock up their checkbooks, look

² Discussion Paper: “Identity Theft: Do Definitions Still Matter” by Julia S. Cheney, August 2005, Payment Cards Center, Federal Reserve Bank of Philadelphia.

at the balances on their bank statements and to look out for themselves rather than to tell them to fear outsiders. Politically it's unfeasible to say that, but there is a lot that individuals can and should be doing to protect ourselves.”³

To reiterate, we, at First Data, agree that consumers should be notified when their personal information has been compromised. Besides distinguishing between forms of fraud, several elements are vital to a fair, effective, national data breach notification standard. These include the ability for breached entities to conduct an internal investigation before notifying consumers and separate notification obligations for entities that own or license data versus entities that maintain data on behalf of the owner or licensor.

Sophisticated attacks upon an entity's information technology system may take time to assess the full extent of the breach. Organizations should have a reasonable period of time in which to investigate their systems before notifying data owners or consumers. In many cases, a breach of the records may not actually lead to card fraud or identity fraud, so consumers benefit less from notification. The federal interagency guidance published in March 2005 by the federal banking regulators echoes this comment.

Secondly, security breach legislation must make an adequate distinction between data owners and data maintainers, which are third party entities (such as First Data), that merely process data on behalf of a data owner. First Data and other processors need this distinction because we often do not have a direct relationship with consumers, and it is far more appropriate for businesses and their customers if the business that owns the data provides the notification to its own customer, rather than a company with which the consumer is most likely unfamiliar. Further, payment processors like First Data may not always have sufficient consumer information to contact the consumer in the event of a breach. For example, as a processor of bank card transactions for retail businesses, we only see the financial piece of the transaction. For most transactions this is simply the date of the transaction, time, amount of sale, card number and card expiration date. Similarly, as a check processor, we may have only bank account, routing and check numbers, as well as the amount of the check at issue but not the consumer's address.

Consumers and businesses are better served if the data owner contacts the consumer directly regarding a security breach instead of third party payment processors like First Data because the data owner has the direct relationship with the consumer. This is the approach used in current practices and federal guidelines. The governing rules for the Visa and MasterCard bankcard associations require that payment processors notify the financial institution if a data processor has a breach. In addition, the federal interagency guidelines for security breach notification direct service providers to notify financial institutions so that those institutions may notify their customers in the manner that is best to meet the needs of the financial institution/customer relationship.⁴

Finally, this issue was well summarized in testimony from Discover Financial Services before the House Financial Services Committee hearing in 2005. “In the event of a data breach affecting credit card information, notification is best handled by the card issuer, not the entity whose

³ LEGALTechnology, The Privacy and Data Protection Legal Reporter, “Cybersecurity Researcher Takes on Internet Fear Factor”, December 26, 2006, <http://www.law.com/tech>.

⁴ 70 Fed. Reg. 15736 (March 29, 2005) (Interagency Guidance [FTC, OTS, FRB, FDIC] on Response Programs for Unauthorized Access to Customer Information and Customer Notice).

security was breached. That entity whose security was compromised must cooperate fully in providing the details necessary to ensure efficient response and notification by the issuer, and to prevent further fraud. But requiring merchants or processors to directly notify affected cardholders may impose an obligation that they cannot readily achieve (since they may not have the necessary consumer contact information), and can needlessly alarm individuals who were not adversely affected by the breach. This might encourage consumers to take steps that are unnecessary (e.g., closing accounts, placing fraud alerts on credit reports). A single notice is the best way to protect credit card users, and card issuers are in the best position to determine whether and when that notice is appropriate.”⁵

5. Education of the Private Sector and Consumers on Safeguarding Data

The Task Force is considering whether there is a need to better educate the private sector on safeguarding information and on what private sector entities should do if they suffer a data breach. Additionally, the Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft, through a national public awareness campaign. Are such education campaigns an appropriate way in which to address the problem of identity theft? If so, what should be the essential elements of these education campaigns for the private sector and consumers?

We believe there is an ongoing need to educate consumers about how to safeguard their personal data. Knowledgeable consumers who take proactive steps to protect their personal information can play an important role in detecting and deterring identity theft. Concomitantly, the FTC has done an excellent job of disseminating educational information to consumers about how to safeguard their data, particularly SSNs. We also support the many state legislatures that have enacted laws prohibiting businesses from publicly posting an SSN, printing SSNs on identification cards, and requiring SSNs to access an Internet site in an unsecured manner. While these are important steps to minimize public use of SSNs, we again caution that more comprehensive restrictions must take into account legitimate business uses of SSNs, especially in the payments sector, to better protect consumers and combat ID theft.

Consumers can also be better educated about the steps to take when they suspect their checks are being used fraudulently:

- 1. Stop payment and close the account.* Call the financial institution that issued your checks to stop payment of the check(s) and close the checking account.
- 2. Ask the financial institution to contact the major check verification companies or contact them directly.* The major check verification companies are: SCAN, a wholly-owned subsidiary of eFunds Corporation (www.consumerdebit.com), TeleCheck (www.telecheck.com) and Fidelity National Information Services, Inc (www.fidelityinfoservices.com). Many retailers and other businesses use check verification companies to reduce bad check losses. Armed with information from check verification companies that checks are the subject of fraud, retailers and other businesses are cautioned not to accept those checks at the point of sale.
- 3. Get a police report.* Call your local police department and tell them that you are a victim of identity theft or fraud and that you want to file a police report.
- 4. File a Federal Trade Commission Complaint.* Although the FTC does not have the authority to bring criminal cases, it makes the complaints available to other federal, state and local law enforcement officials worldwide.

⁵ Statement of Carlos Minetti, Discover Financial Services before the Subcommittee on Oversight and Investigations of the Committee on Financial Services, United States House of Representatives, July 21, 2005.

Finally, we believe there is a role for the federal government to play in educating the private sector about the need to safeguard consumers' personal information. However, there is an equal or greater need for the federal government to educate the public sector (e.g. local and state governments, institutions of higher learning) about the need to protect consumer's personal information.

***IV. Ability of Law Enforcement to Receive Information from Financial Institutions
Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force is considering: (b) whether relevant federal law enforcement agencies should continue discussions with the financial services industry to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft.***

Safeguarding sensitive data from unauthorized access is a top priority at First Data, and our reputation hinges on effecting payment transactions safely, securely, and reliably. However, success in the daily battle against ID theft requires the cooperation of local, state and federal law enforcement, foreign governments, as well as other players within the financial services industry and the merchant/retail industry.

Thank you for the opportunity to provide comments. Please feel free to contact me with any questions, comments, or concerns you may have.

Sincerely,
Joe Samuel
Senior Vice President, Public Policy
First Data Corporation
(p) 303-967-7195
(e) joe.samuel@firstdatacorp.com